Mbed TLS Tech Forum

https://github.com/Mbed-TLS

Janos Follath

2025-08-11

Recent community activity (thank you!)

- tls#10347 aphroteus - [3.6] Fix a build failure that occurs in environments using Code Page 950
- tls#10140 irwir - Use native socket type on Windows
- tls#10202 LoveKarlsson - [3.6] Fix alignment problems with IAR and Zephyr
- tls#9542 manoel-serafim - Performance Enhancements and Memory Footprint Reduction in mbedtls_internal_sha(256|512)_process_c()
- merged: tls#5837 robert-shade - Allow building as a subdir
- tls#10318 keith-packard - Avoid invalid gcc 14.3 warning about array bounds in mbedtls_xor
- tls#10322 yamt - benchmark.c: Add a mbedtls_timing_hardclock variation with xtensa CCOUNT
- frame#193 irwir - Exclude "WIN32_LEAN_AND_MEAN" from name check
- crypto#411 aphroteus - Fix a build failure that occurs in environments using Code Page 950
- crypto#410 LoveKarlsson - Made alignment typedefs more robust for IAR
- crypto#403 amjoul01 - psa: mac: only call memset if key_length is less than block size
- crypto#262 irwir - Add winsock2 header into build_info.h
- crypto#391 keith-packard - Avoid invalid gcc 14.3 warning about array bounds in mbedtls_xor
- merged: crypto#389 ariwo17 - Remove PKCS12 module (MBEDTLS_PKCS12_C) and related test code
- crypto#390 yamt - benchmark.c: Add a mbedtls_timing_hardclock variation with xtensa CCOUNT

Recent community activity (thank you!)

Valerio @Nordic

- merged: tls#10344 valeriosetti - [development] Remove 224-bit curves & Remove 192-bit curves from TLS & X.509 (2/3)
- tls#10041 valeriosetti - [development] Make mbedtls_psa_register_se_key usable with opaque drivers
- tls#10333 valeriosetti - [development] Migrate from mbedtls_pk_can_do_ext to mbedtls_pk_can_do_psa (2/2)
- merged: tls#10329 valeriosetti - [development] Define MBEDTLS_PK_ALG_ECDSA (1/2)
- merged: frame#197 valeriosetti - [framework] Remove 224-bit curves (1/3)
- frame#145 valeriosetti - [framework] Make mbedtls_psa_register_se_key usable with opaque drivers
- crypto#408 valeriosetti - [tf-psa-crypto] Remove 224-bit curves (3/3)
- crypto#394 valeriosetti - [tf-psa-crypto] Implement mbedtls_pk_can_do_psa (improved mbedtls_pk_can_do_ext) (1/2)
- crypto#191 valeriosetti - [tf-psa-crypto] Make mbedtls_psa_register_se_key usable with opaque drivers
- merged: crypto#401 valeriosetti - include: pk: use PSA_WANT instead of ECDSA_DETERMINISTIC for PK_ALG_ECDSA
- merged: crypto#388 valeriosetti - [tf-psa-crypto] Define MBEDTLS_PK_ALG_ECDSA (2/2)
- merged: crypto#308 valeriosetti - [tf-psa-crypto] PK: try storing all private RSA keys in PSA (3/3)

Major activities within core team

https://github.com/orgs/Mbed-TLS/projects/18

- TF-PSA-Crypto
  - First standalone components are now running in the CI
- Mbed TLS 4.0/TF-PSA-Crypto 1.0
  - Making low level crypto functions internal
  - Removing legacy types from public non-PSA interfaces
  - Released 4.0/1.0 beta for early evaluation

Release Timeline

- 1.0/4.0 currently aiming for September 2025
- 3.6 LTS supported until early 2027
  - 3.6.1 (Aug 2024): mostly fixes related to TLS 1.3
  - 3.6.2 (Oct 2024): security fix
  - 3.6.3 (March 2024): supports a PSA key store in builds without malloc
  - 3.6.4 (June 2024): GCC 15 support, other bug and security fixes

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు